ONR Final Technical Report
Award #N00014-99-0150
1/1/99 - 12/31/06
"Collaborative Research on Systems and Security"

NAME OF PI: Michael Mislove

UNIVERSITY/Contractor:
Tulane University

TITLE OF PROJECT: Collaborative Research on Systems and Security

GRANT/CONTRACT/WORK REQUEST NUMBER:
N00014-99-1-0150

1. Papers published in referred journals (TITLE; JOURNAL):

1) A truly concurrent semantics for a process algebra using resource pomsets, Special Issue of Theoretical Computer Science dedicated to Maurice Nivat, TCS **281** (2002), pp. 369--422.
2) Measuring the probabilistic powerdomain, Theoretical Computer Science **312** (2004), 99-119, with K. Martin and J. Worrell
3) A simple process algebra based on atomic actions with resources, Mathematical Structures for Computer Science **14** (2004), 1—55. With J. Worrell
4) Domain theory, testing and simulation for labeled Markov processes, Theoretical Computer Science **333** (2005), 171—197, with F. van Breugel, J. Ouaknine and J. Worrell

2. Papers published in conference proceedings (TITLE; JOURNAL):

1) Local dcpos, local cpos and local completions, Proceedings of MFPS 15, ENTCS **20** (1999).
2) Trace theory and state explosion, Proceedings of PDPTA 1999, 288—294
3) A truly concurrent semantics for a simple parallel programming language, Proceedings of CSL 1999, Lecture Notes in Computer Science (1999), 515—529, with P. Gastin
4) Models supporting nondeterminism and probabilistic choice, Proceedings of IPDPS, LNCS (2000), 993—1000
5) Nondeterminism and probabilistic choice: Obeying the laws, Proceedings of CONCUR 2000, LNCS (2000), 350—364
6) Measuring the probabilistic power domain, ICALP 2002, Lecture Notes in Computer Science **2380** (2002), pp. 463-475 (with K. Martin and J. B. Worrell).
7) Timed CSP = closed timed automata. Proceedings of EXPRESS `02, ENTCS **68(2)**, 2002, J. Ouaknine and J. Worrell.
8) Testing Labelled Markov Processes. Proceedings of the 29th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science **2380** (2002), F. Van Breugel, S. Shalit and J. Worrell.
9) An intrinsic characterization of approximate probabilistic bisimilarity, Proceedings of FoSSACS 2003, LNCS (2003), 200-215, with F. van Breugel, J. Ouaknine and J. Worrell
10) Axioms for probability and nondeterminism, Proceedings of EXPRESS 2004, ENTCS **96** (2004), 7—28, with J. Ouaknine and J. Worrell.
11) Duality for labeled Markov processes, Proceedings of FoSSACS 2004, LNCS (2004), 393—407, with J. Ouaknine, D. Pavlovic and J. Worrell
12) Discrete random variables over domains, Proceedings of ICALP 2005, LNCS (2005), 1006—1017
13) On combining probability and nondeterminism, Proceedings of 25 years of Algebraic Process Theory, ENTCS **162** (2006), 261—265
14) Testing semantics: Connecting processes and process logics, Proceedings of AMAST 2006, LNCS **4019** (2006), 308--322

3. Books or Book chapters published (TITLE; AUTHORS/EDITORS; PUBLISHER):

1) Continuous Lattices and Domains, Cambridge University Press, 2003, 581pp, with G. Gierz, K. Hofmann, K. Keimel, J. Lawson and D. Scott

4. Proceedings Edited (TITLE; AUTHORS/EDITORS; PUBLISHER):

1) Proceedings of MFPS 15, ENTCS **20** (1999), with S. Brookes, A. Jung and A. Scedrov.
2) Proceedings of Conference on Modern Algebra, Theoretical Computer Science **249** (2001), with K. Keimel and C. Tsinakis
3) Proceedings of MFPS 2001, ENTCS **45** (2001), with S. Brookes.
4) Proceedings of MFPS 12, Theoretical Computer Science **278** (2002), with S. Brookes
5) Proceedings of MFPS 14 and MFPS 16, Theoretical Computer Science **315** (2004)
6) Proceedings of Clifford Lectures and MFPS 18, Theoretical Computer Science **357** (2006), with S. Artemov.
7) Proceedings of MFPS 21, ENTCS **155** (2006), with M. Escardo and A. Jung
8) Proceedings of MFPS 22, ENTCS **158** (2006), with S. Brookes.

5. Patents (ANNOTATE EACH WITH FILED OR GRANTED):

None

8. Presentations (INVITED):

1) Models supporting nondeterminism and probabilistic choice, Fifth International Workshop on Formal Methods for Parallel Programming, Cancun, MX, May, 2000
2) Seminar on Topology and Computer Science, Schloss Dagstuhl, Germany, June, 2000
3) Universite de Paris VII, June, 2000
4) Nondeterminism and probabilistic choice: Obeying the laws, CONCUR 2000, Penn State University, August, 2000
5) Engineering Automation for Software Intensive System Integration Workshop, Monterey, CA, June, 2001
6) Universite de Paris VII, June, 2001
7) Special Session on Topology and Computer Science, Summer Topology Conference, CCNY, New York, July, 2001 (co-organizer)
8) Measuring the probabilistic power domain, Seminar on Topology and Computer Science, Schloss Dagstuhl, Germany, May, 2002.
9) Colimits in categories of topological and ordered spaces, Summer Topology Conference, Auckland, New Zealand, July, 2002.
10) Plenary Lecture, Nineteenth Conference on the Mathematical Foundations of Programming Semantics, Montreal, CA, March, 2003
11) Workshop on Domain-theoretic Models of Probability, Bellairs Research Station, Barbados, April, 2003
12) Seminar, University of Birmingham, UK, June, 2003
13) Conference Honoring John Pym, University of Sheffield, UK, June, 2003
14) Workshop on Interoperability, Pervasive computing and Security, Harpers Ferry, WV, September 2003
15) Invited Lecture, Workshop Honoring Klaus Keimel, Technische Universitaet Darmstadt, Germany, September, 2004
16) Invited lecture, Workshop on Ordered Structures and Homeland Security, DIMACS, September, 2004
17) ONR AASU Workshop, Savannah, GA, September, 2004
18) Topology and Computer Science Seminar, University of Oxford, UK, May, 2005
19) Discrete random variables over domains, ICALP, Lisbon, PT July, 2005
20) Computer Science Seminar, CUNY Graduate School, November, 2005
21) Variations on an interval domain theme, Conference Honoring Peter Collins and G. M. Reed, University of Oxford, UK, August, 2006
22) From predicates to probabilistic systems, Invited talk, Conference on Emerging Trends in Concurrency, LIX, Ecole Polytechnique, Paris, November, 2006

8. **Presentations (CONTRIBUTED):**

1) Models of probability and nondeterminism, Sixteenth Workshop on the Mathematical Foundations of Programming Semantics, Hoboken, NJ, April, 2000
2) Measuring the probabilistic power domain, ICALP 2002, Malaga, Spain, June, 2002
3) Testing Labelled Markov Processes. ICALP 2002, Malaga, Spain, June, 2002
4) Timed CSP = closed timed automata, EXPRESS '02, Grenoble, France, April, 2002

8. **Summary of Research Accomplishments:**

There are two areas where the research conducted under this grant was focused: (1) research on models of concurrency, and in particular on true concurrency, and (2) models for probabilistic choice. In the first area, we collaborated with Professor Paul Gastin, then of the Universite de Paris VII, over a period of years on devising domain-theoretic models to support true concurrency. This approach to modeling concurrent computation differs from the usual approach, where parallel composition is modeled by synchronization and interleaving of non-synchronized actions. In true concurrency, the approach is different, with an attempt to model actions occurring concurrently, rather in a specified order. The results of this research are reported in the journal papers 1) and 3) above. The summary of the results are that we devised a denotational model for a simple parallel programming language that supports prefixing, sequential composition, hiding, restriction, parallel composition using true concurrency, and recursion. We also showed that the denotational model is fully abstract with a natural operational model for the process calculus we devised, where one observes only unsynchronized atomic actions.

The second area of research focused on models for probability. Our interest in this area was inspired by results of our colleague A. W. Roscoe, who showed that there is no information flow in a system where Low's view of the system is "deterministic". The idea was to devise a more comprehensive model where probabilistic choice could replace nondeterminism, thus allowing a differentiation between the choices of the system and those of the users.

Our first results along this line provided a model for probabilistic choice that also supports nondeterminism, in a setting in which the expected laws for both operations are obeyed in the model. This work is reported in paper 3) under papers in conference proceedings. The model was also independently discovered by R. Tix. This model is quite interesting, and it is fully understood in terms of the domain-theoretic structure. Unfortunately, repeated attempts by this investigator, both alone and in collaboration with some of the leading experts in CSP, failed to devise a model for CSP that supports probabilistic choice in which the expected laws of CSP are observed. We now believe such a model is not possible.

At the same time we were investigating the interplay of nondeterminism and probabilistic choice, we also were inspired to look at whether the probabilistic power domain would support a measurement. The intuition is that such a measurement should be given by integration against a measurement on the underlying domain, and indeed this turned out to be the case. This work, which was joint with my former PhD student K. Martin and with my postdoc J. Worrell, is reported in the journal paper 2) and the conference proceedings 4) above. The main application of the results reported in those papers was a much more intuitive proof of the existence of an invariant measure on a weakly hyperbolic iterated function system. Remarkably, we have recently found new applications of this measurement theory in our attempts to devise domain-theoretic models of the probabilistic input/ouput automata of Lynch and her collaborators.

Our research on probabilistic models then turned to work originated by Larsen and Skou, who considered how to define probabilistic bisimulation on probabilistic transition systems. Their work focused on case of a finite state space, and Panangaden and his collaborators devised generalizations to the setting of an analytic state space. The general setting is what are called labeled Markov processes, in which one has a state space, a set of actions, and a transition system in which executing an action in any state results in a probability distribution over the next states the system will then be in. Our results in this area are reported in the journal paper 4) and the conference papers 6) – 9) listed above. The initial results focused on trying to give a better characterization of both probabilistic simulation and bisimulation, and the approach used was one implemented by testing processes against actions they might perform. This later led to results about characterizing the processes intrinsically, and this resulted in a dualty theory for these processes. The key insight here was the realization that just as actions can test processes, processes can test actions and sequences of actions. The duality theorem shows that each labeled Markov process is characterized up to probabilistic bisimulation by the tests it can perform, and these tests give rise to a real C*-algebra that forms the dual of the Markov process. These results have led to further results reported in the conference paper 14) above, in which this testing philosophy is pushed even further and which shows promise for giving a very general characterization of the equivalence of computational processes.

Another facet of the work on labeled Markov processes is reported in the conference paper 8) above, in which the earlier work on probability and nondeterminism was picked up again in the context of labeled Markov processes. The main result shows how the labeled Markov process theory gives rise to an operational model for a simple process calculus which extends Milner's CCS with probabilistic choice, and in which this operational model qua bisimulation relation has the earlier domain-theoretic model for nondeterminism and probabilistic choice as a fully abstract denotational model.

The final aspect of research to report on this contract is reported in the conference paper 19). Here we took up the ideas of Daniele Varacca, who PhD thesis devised more general models for probabilistic choice and nondeterminism that are better-behaved than the usual ones, because they don't introduce any relationship between probabilistic choice and nondeterministic choice, as happens in the model reported in paper 3) under conference papers. Varaccca's presentation is somewhat arcane, and even though he does present domain-theoretic models, their internal structure is far from transparent. We worked on providing a more approachable path to constructing his models, and in the processes, we devised the first model for probabilistic choice based on random variables, rather than probability measures (although there is usually no distinctions between these constructs, in this setting the algebraic operations lead to distinctions). The results also gave rise to the first model for probabilistic choice that is known to leave a cartesian closed category of continuous domains invariant. This opens the door to devising a model of the lambda calculus that also supports probabilistic choice, something long a goal in semantics.

7. Honors (Presidential YIP, elections to Fellow status in major scientific society; appointed editor of scientific journal, elected NAS/NAE/IOM, awarded medal by scientific society, Chairman of scientific meeting, etc):

1) Editor-in-Chief of *Theoretical Computer Science* for the series *Electronic Notes in Theoretical Computer Science*, 2001 – 2003.
2) Member, Council of the European Association for Theoretical Computer Science, 2001 -- 2006
3) Steering Committee, Summer Topology Conference series., 2001—2004.
4) Visiting Professor, University of Paris VII, June, 2000, 2001, 2002.
5) Visiting Professor, University of Udine, Italy, May, 2003.
6) Honored for contributions to MFPS at the MFPS 2004 meeting, Pittsburgh. PA, April, 2004.
7) Invited participant, CSFW, Asilomar, CA, June, 2003
8) Invited participant, CSFW, Aix en Provence, France, Juune, 2005
9) Listed in *Who's Who in America, Who's Who in Science and Engineering.*
10) Named Pendergraft Herbert Buchanan Professor, Tulane University, 2006 –

8. Number of graduate students:
2

9. Number of Post-doctoral students:
2

10. Number of undergraduate students supported:
0

11. Number of under-represented members by group:
1